AMENDMENTS TO THE CLAIMS

Please cancel claim 16 without prejudice Kindly amend claims 1, 6-8, 17, 20-23, and 26 as shown in the following listing of claims. The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

fetch logic, disposed within a microprocessor, configured to receive a ~~cryptographic instruction~~single atomic cryptographic instruction as part of an instruction flow executing on said microprocessor, wherein said cryptographic instructionsingle atomic cryptographic instruction prescribes one of the cryptographic operations, and wherein said ~~cryptographic instruction~~single atomic cryptographic instruction prescribes that a provided cryptographic key be expanded into a corresponding key schedule for employment during execution of said one of the cryptographic operations;

translation logic, coupled to said fetch logic, configured to translate said single atomic cryptographic instruction into a sequence of micro instructions that directs said microprocessor to perform said one of the cryptographic operations;

keygen logic, disposed within said microprocessor and operatively coupled to said cryptographic instructionsingle atomic cryptographic instruction, configured to direct said microprocessor to expand said provided cryptographic key into said corresponding key schedule; and

execution logic, disposed within said microprocessor and operatively coupled to said keygen logic, configured to expand said provided cryptographic key into said corresponding key schedule. said execution logic comprising:

a cryptography unit, configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit.

2. (Original) The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

3. (Original) The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

4. (Original) The apparatus as recited in claim 1, wherein said provided cryptographic key is stored in memory.

5. (Original) The apparatus as recited in claim 1, wherein said corresponding key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm.

6. (Currently Amended) The apparatus as recited in claim 1, wherein said keygen logic is configured to interpret a key generation field within a control word which is referenced by said cryptographic instructionsingle atomic cryptographic instruction.

7. (Currently Amended) The apparatus as recited in claim 1, wherein said cryptographic instructionsingle atomic cryptographic instruction is prescribed according to the instruction format for execution on an x86-compatible microprocessor.

8. (Currently Amended) The apparatus as recited in claim 1, wherein said cryptographic instruction~~single atomic cryptographic instruction~~ implicitly references a plurality of registers within said ~~computing device~~microprocessor.

9. (Original) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of said plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished.

10. (Previously Presented) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks.

11. (Original) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a first register, wherein contents of said first register indicate a number of text blocks within a plurality of input text blocks.

12. (Original) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

13. (Original) The apparatus as recited in claim 12, wherein said cryptographic key data comprises said provided cryptographic key.

14. (Previously Presented) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory, said first location comprising an initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations.

15. (Original) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations, and wherein said control word comprises:

a keygen field, configured to specify that said provided cryptographic be expanded into said corresponding key schedule be employed during execution of said one of the cryptographic operations.

16. (Cancelled)

17. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

a cryptography unit within disposed within execution logic in a microprocessor, configured to execute one of the cryptographic operations responsive to receipt by said microprocessor of a ~~cryptographic instructions~~single atomic cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said ~~cryptographic~~ instructionsingle atomic cryptographic instruction is fetched from memory by fetch logic in said microprocessor, and wherein said ~~cryptographic~~ instructionsingle atomic cryptographic instruction also prescribes that a cryptographic key be expanded into a corresponding key schedule to be employed when executing said one of the cryptographic operations, and wherein translation logic in said microprocessor translates said single atomic cryptographic instruction into a sequence of micro instructions that directs said microprocessor to perform said one of the cryptographic operations; and

keygen logic, operatively coupled to said cryptography unit, configured to direct said microprocessor to perform said one of the cryptographic operations and to expand said cryptographic key into said corresponding key schedule.

18. (Original) The apparatus as recited in claim 17, wherein said cryptographic key is stored in memory.

19. (Original) The apparatus as recited in claim 17, wherein said corresponding key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm.

20. (Currently Amended) The apparatus as recited in claim 17, wherein said keygen logic is configured to interpret a key generation field within a control word which is referenced by said cryptographic instructionsingle atomic cryptographic instruction.

21. (Currently Amended) The apparatus as recited in claim 17, wherein said cryptographic instructionsingle atomic cryptographic instruction is prescribed according to the instruction format for execution on an x86-compatible microprocessor.

22. (Currently Amended) A method for performing cryptographic operations, the method comprising:

within a microprocessor, fetching a cryptographic instructionsingle atomic cryptographic instruction from memory that prescribes expansion of a cryptographic key into a corresponding key schedule for employment during execution of one of a plurality of cryptographic operations, and translating the single atomic cryptographic instruction into a sequence of micro instructions that direct the microprocessor to perform the one of the plurality of cryptographic operations; and

via a cryptography unit disposed within execution logic inwithin the microprocessor, ~~executing the cryptographic instruction and~~ expanding the cryptographic key into the corresponding key schedule.

23. (Currently Amended) The method as recited in claim 22, wherein said fetching comprises:

via a field within a control word that is referenced by the ~~cryptographic instruction~~single atomic cryptographic instruction, specifying expansion of the cryptographic key into the corresponding key schedule.

24. (Original) The method as recited in claim 22, wherein said expanding comprises:

loading the cryptographic key from memory.

25. (Original) The method as recited in claim 22, wherein the corresponding key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm.

26. (Currently Amended) The method as recited in claim 22, wherein said fetching comprises:

prescribing the cryptographic instructionsingle atomic cryptographic instruction according to the instruction format for execution on an x86-compatible microprocessor.